Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:05:02 UTC

Tool: MoonBounce

Names	MoonBounce
Category	Malware
Type	Backdoor, Rootkit
Description	(Kaspersky) The UEFI implant, which was detected in spring 2021 , was found to have been incorporated by the attackers into the CORE_DXE component of the firmware (also known as the DXE Foundation), which is called early on at the DXE (Driver Execution Environment) phase of the UEFI boot sequence. Among other things, this component is responsible for initializing essential data structures and function interfaces, one of which is the EFI Boot Services Table – a set of pointers to routines that are part of the CORE_DXE image itself and are callable by other DXE drivers in the boot chain.
Information	<https://securelist.com/moonbounce-the-dark-side-of-uefi-firmware/105468/>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/win.moonbounce>

Last change to this tool card: 27 December 2022

Download this tool card in JSON format

All groups using tool MoonBounce

Changed	Name	Country	Observed	
APT groups				
	APT 41		2012-Jul 2025	

1 group listed (1 APT, 0 other, 0 unknown)